PTO 08-7596

CC=JP
DATE=20020621
KIND=Kokai
PN=2002175224

NETWORK CONNECTION SYSTEM AND DEVICE
[Nettowaku Setsuzoku Shisutemu Oyobi Sochi]

Yoichi Shirakawa

UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. SEPTEMBER 2008
TRANSLATED BY Schreiber Translations, Inc.

PUBLICATION COUNTRY	(10):	Japan
DOCUMENT NUMBER	(11):	2002175224
DOCUMENT KIND	(12):	Kokai
PUBLICATION DATE	(43):	20020621
APPLICATION NUMBER	(21):	200371240
APPLICATION DATE	(22):	20001206
INTERNATIONAL CLASSIFICATION	(51):	G 06 F 13/00, H 04 L 12/46, 12/66
PRIORITY COUNTRY	(33):	
PRIORITY NUMBER	(31):	
PRIORITY DATE	(32):	
INVENTOR(S)	(72):	Yoichi Shirakawa
APPLICANT(S)	(71):	NEC Corporation
DESIGNATED CONTRACTING STATES	(81):	
TITLE	(54):	NETWORK CONNECTION SYSTEM AND DEVICE
FOREIGN TITLE	[54A]:	Nettowaku Setsuzoku Shisutemu Oyobi Sochi

/2[1]

Claims

1. A network connection system, characterized by the fact that in a network connection system equipped with an internal network having several computers and a network connection device for connecting said internal work with an external network, the above-mentioned network connection device is equipped with a switching means in which the other end is connected to the above-mentioned external network and the above-mentioned internal network and the above-mentioned external network are switched to any of a substantial connection state and a substantial cut-off state; and a control means that switches the above-mentioned switching means to the substantial connection state or the substantial cut-off state in accordance with the establishment of prescribed conditions.

2. The network connection system of Claim 1, characterized by the fact that it is further equipped with a firewall that checks the access to the above-mentioned network from the above-mentioned external network and

[1] Numbers in the margin indicate pagination in the foreign text.

controls the access to the internal network if said access is an illegal access.

3. The network connection system of Claim 1, characterized by the fact that the above-mentioned internal network and the above-mentioned external network are connected via the firewall including an alarm generation means for generating an alarm if there is an illegal access to the above-mentioned internal network from the above-mentioned external network; the above-mentioned network connection device is realized as a function in the above-mentioned firewall; and the above-mentioned control means sets the above-mentioned switching means to a substantial cut-off state if the above-mentioned alarm generation means generates an alarm.

4. A network connection device, characterized by the fact that in a network connection device for connecting an internal network having several computers to an external network, it is equipped with a switching means in which the other end is connected to the above-mentioned external network and the above-mentioned internal network and the above-mentioned external network are switched to any of a substantial connection state and a substantial cut-off state; and a control means that switches the above-mentioned switching means to the substantial connection

state or the substantial cut-off state in accordance with the establishment of prescribed conditions.

5. The network connection device of Claim 4, characterized by the fact that the above-mentioned switching means and the above-mentioned control means are realized as a function of a firewall including an alarm generation means for generating an alarm if there is an illegal access to the above-mentioned internal network from the above-mentioned external network; and the above-mentioned control means sets the above-mentioned switching means to a substantial cut-off state if the above-mentioned alarm generation means generates an alarm.

6. The network connection device of Claim 4 or 5, characterized by the fact that the above-mentioned control means monitors the generation of a prescribed event in the above-mentioned internal network and switches the above-mentioned switching means to a substantial connection state or a substantial cut-off state in accordance with the generation of said prescribed event.

7. The network connection device of Claims 4-6, characterized by the fact that the above-mentioned control means switches the above-mentioned switching means to a substantial connection state or a substantial cut-off state

as the time clocked by a clock means becomes a prescribed time.

Detailed explanation of the invention

[0001]

(Technical field of the invention)

The present invention pertains to a network connection system and device for connecting an internal network such as LAN (Local Area Network) and an external network such as WAN (Wide Area Network).

[0002]

(Prior art)

Recently, many computers have been connected in a certain shape by a network and used, however the prevention of an illegal access to each computer has become a big problem. In particular, in a network system in which an internal network such as LAN and an external network such as WAN starting with Internet are connected, generally, a firewall is installed between the internal network and the external network, and each computer is prevented from being illegally accessed from the external network by the authentication of the firewall or filtering.

[0003] On the other hand, even in the network connection system via the firewall, basically, each computer connected to the internal network is always connected to the external network. For this reason, illegal accesses from the external network could not completely cut off. Accordingly, as a technique for preventing an illegal access from the outside in each computer, a network interface module with a security switch is proposed in Japanese Kokai Patent Application No. 2000-10877.

[0004] Figure 4 is a block diagram showing a network interface module with a security switch described in Japanese Kokai Patent Application No. 2000-10877. As shown in the figure, a network interface module 101 is installed in accordance with computers 105 by a one-to-one correspondence and consists of a network face 102 and a power source interface 103 including a security switch 104.

[0005] A power of the network interface module 101 is supplied from a power source 107 in the computers 105. If the CPU 10-6 stops the supply of the power from the power source 107, the security switch 104 is turned off, and the

/3

network interface 102 cannot be operated. Thus, the computers 105 cannot be accessed from an external network, so that an illegal access to the computers 105 can be prevented.

[0006]

(Problems to be solved by the invention)

However, in the technique described in Japanese Kokai Patent Application No. 2000-10877, the network interface module 101 must be installed in accordance with each computer 105. On the other hand, in the system in which the internal network and the external network are connected, an illegal access to the computers 105 from the internal work cannot be considerably considered. For such an illegal access that can be little considered, a redundant constitution in each of the computers 105 is useless in terms of space and cost.

[0007] Also, in the computers connected to the internal network, furthermore, the external network, usually, data are frequently exchanged in the internal network, whereas the exchange of data with the external connection is overwhelmingly less. For this reason, if the network interface module 101 is installed for each of the computers 105 and each of the computers rejects the access, like Japanese Kokai Patent Application No. 2000-10877, there is a possibility that a trouble is caused in the exchange of data in only the internal network.

[0008] The purpose of the present invention is to provide network access system, etc., that prevent computers connected to an internal network from an illegal access from an external network and can effectively exchange data in the internal network.

[0009]

(Means to solve the problems)

In order to achieve the above-mentioned purpose, the network connection system of a first viewpoint of the present invention is characterized by the fact that in the network connection system equipped with an internal network having several computers and a network connection device for connecting said internal work with an external network, the above-mentioned network connection device is equipped with a switching means in which the other end is connected to the above-mentioned external network and the above-mentioned internal network and the above-mentioned external network are switched to any of a substantial connection state and a substantial cut-off state; and a control means that switches the above-mentioned switching means to the substantial connection state or the substantial cut-off state in accordance with the establishment of prescribed conditions.

[0010] In the above-mentioned network connection system, the control means sets the switching means to a substantial cut-off state, so that the internal network cannot be accessed from the external network. Thereby, even if the switching means is set to a substantial cut-off state, the computers in the internal network maintain an interconnection state, and no trouble is caused in the exchange of the data in the internal network.

[0011] The above-mentioned network connection system is further equipped with a firewall that checks the access to the above-mentioned network from the above-mentioned external network and controls the access to the internal network if said access is an illegal access.

[0012] In the above-mentioned network connection system, the above-mentioned internal network and the above-mentioned external network may also be connected via the firewall including an alarm generation means for generating an alarm if there is an illegal access to the above-mentioned internal network from the above-mentioned external network. In this case, the above-mentioned network connection device can be realized as a function in the above-mentioned firewall, and the above-mentioned control means can set the above-mentioned switching means to a substantial cut-off state if the above-mentioned alarm generation means generates an alarm.

[0013] As shown in these constitutions, with the use of the firewall in addition to the switching means, an illegal access to the internal network from the external network can be more reliably prevented, so that a higher-security system can be constructed.

[0014] In order to achieve the above-mentioned purpose, the network connection device of a second viewpoint of the present invention is characterized by the fact that in the network connection device for connecting an internal network having several computers to an external network, it is equipped with a switching means in which the other end is connected to the above-mentioned external network and the above-mentioned internal network and the above-mentioned external network are switched to any of a substantial connection state and a substantial cut-off state; and a control means that switches the above-mentioned switching means to the substantial connection state or the substantial cut-off state in accordance with the establishment of prescribed conditions.

[0015] In the above-mentioned network connection device, the above-mentioned switching means and the above-mentioned control means may also be realized as a function of a firewall including an alarm generation means for generating an alarm if there is an illegal access to the above-mentioned internal network from the above-mentioned external network. In this case, the above-mentioned control means can set the above-mentioned switching means to a substantial cut-off state if the above-mentioned alarm generation means generates an alarm.

[0016] In the above-mentioned network connection device, the above-mentioned control means can monitor the generation of a prescribed event in the above-mentioned internal network and switch the above-mentioned switching means to a substantial connection state or a substantial cut-off state in accordance with the generation of said prescribed event.

[0017] In the above-mentioned network connection device, /4 the above-mentioned control means, furthermore, can also switch the above-mentioned switching means to a substantial connection state or a substantial cut-off state as the time clocked by a clock means becomes a prescribed time.

[0018]

(Embodiments of the invention)

Next, embodiments of the present invention are explained referring to the figures.

[0019] Figure 1 is a block diagram showing the constitution of the network connection system of this embodiment. As shown in the figure, in the network connection system, several computers 11 are connected to a LAN 1 as an internal network. The LAN 1 is connected to a line switch part 21 and a control part 22. The line switch part 21 and the control part 22 are included in the internal network in a broad sense. The other end of the line switch 21 is connected to a WAN 3 as an external network. Also, specifically, the LAN 1 can be Intranet, and the WAN 3 can be Internet.

[0020] The line switch part 21 switches a connection state or a cut-off state between the LAN 1 and the WAN 3 based on a control signal being sent from the control part 22. The control part 22 generates and output a control signal for switching the state of the line switch part 21 based on the control signal being obtained from the LAN 1.

[0021] The control part 22, for example, can be realized by a line board being connected to the LAN 1, a personal computer for controlling the line switch part 21, etc. In this case, the line switch part 21 may also be a cable switch for physically turning on/off the LAN 1 and the WAN 3 by a serial signal. Also, the line switch part 21 and the control part 22 may be realized by a special hardware device. In this case, an interface being connected to the LAN 1 and an interface being connected to the WAN 3 may also be provided.

[0022] Next, the operation of the network connections system is explained. Here, in an ordinary state, the line switch part 21 is set to a cut-off state.

[0023] When an event in which the LAN 1 and the WAN 3 are to be connected, for example, an event in which any of the computers 11 accesses a computer device on the WAN 3 and obtains data is generated, said computer 11 informs the WAN 3 of the access. Based on this information, the control part 22 sends a control signal to the line switch part 21 and switches the line switch part 21 to a connection state.

[0024] After the line switch part 21 is set to a connection state, said computer 11 accesses the computer device on the WAN 3 and obtains data from it. After the acquisition of the data is finished, said computer 11 informs the control part 22 of the end of the access to the WAN 3. Based on this information, the control part 22 sends the control signal to the line switch part 21 and switches the line switch part 21 to a cut-off state.

[0025] On the other hand, when the computer device on the WAN 3 tries to access any of the computers 11 in the LAN 1, since the line switch part 21 is usually set to a cut-off state, the computer device cannot access the computer 11. In this case, since the computers 11 in the LAN 1 are in a connection state, they can freely exchange data with each other.

[0026] As explained above, in the network connection system of this embodiment, if the control part 22 sets the line switch part 21 to a cut-off state, the computers 11 in the LAN 1 cannot be accessed from the WAN 3. For this reason, if the computer 11s in the LAN 1 do not need to exchange data with the WAN 3 as an external network, since the line switch part 21 may be set to an entirely cut-off state, the computers 11 in the LAN 1 can be prevented from being illegally accessed from the WAN 3.

[0027] Also, even if the line switch part 21 is in a cut-off state, the computers 11 in the LAN 1 can always maintain a connection state. For this reason, the processing in the LAN 1 can be efficiently carried out without causing a trouble in the exchange of data of the computers 11 in the LAN 1.

[0028] The present invention is not limited to the above-mentioned embodiment but can be variously modified and applied. Next, modified patterns of the above-mentioned embodiment applicable to the present invention are explained.

[0029] In the above-mentioned embodiment, the control part 22 has switched the line switch part 21 to a connection state or a cut-off state. On the contrary, the line switch part 21 can be switched by an event generated in the WAN 3 as an external network. Originally, the event generated in the WAN 3 is transferred to the control part 22, only when the line switch 21 is set to a connection state, and the control part 22 can switch the line switch 21 from a connection state to a cut-off state at an appropriate timing based on the event generated in the WAN 3.

[0030] Also, the connection state and the cut-off state of the line switch 21 of the control part 22 can be switched by the clocking time of a timer. For example, synchronous application, mail and news delivery, file transfer and backup, etc., can be carried out, even if the connection is not always made. Accordingly, the line switch part 1 may be set to a connection state in a preset time zone in accordance with the clocking time of the timer, and the data may be exchanged. Also, the timer may be provided to /5 the control part 22 itself or may exist at the outside of the control part 22 and input time information into the control part 22.

[0031] In the above-mentioned embodiment, the LAN 1 and the WAN 3 have been connected only via the line switch part 21. On the contrary, a network connection system with a constitution in which a firewall is used together can also be constituted in the connection of the LAN 1 and the WAN 3.

[0032] Figure 2 is a block diagram showing the constitution of a network connection system with another constitution in which a firewall is used together. In this network connection system, a firewall 23 is further installed between the line switch part 21 and the LAN 1. Originally, the position of the firewall 23 may exist between the line switch part 21 and the WAN 3.

[0033] In the network system of Figure 2, it is assumed that there is an illegal access in the computers 11 in the LAN 1 from the WAN 3. Here, if the line switch part 21 is set to a connection state, this illegal access reaches the firewall 23. Next, the firewall 23 applies a filter to the access from the WAN 3, however due to the illegal access, the access cannot be transferred to the computers 11 in the LAN. With this constitution, the prevention of an illegal access to the computers 11 in the LAN 1 from the WAN 3 is reinforced, and a higher-security system can be constructed, compared with the system shown in the above-mentioned embodiment.

[0034] Figure 3 is a block diagram showing the constitution of a network connection system with another constitution in which a firewall is used together. In this network connection system, the LAN 1 and the WAN 3 are connected via the firewall 2, and the line switch 21 and the control part 22 are realized as a function of the firewall 2. The firewall 2 includes an alarm generation part 24 for generating an alarm if there is an illegal access to the computers 11 in the LAN 1 from the WAN 3.

[0035] Here, when the alarm generation part 24 generates an alarm, the control part 22 sends a control signal to the line switch part 21 so that the LAN 1 and the WAN 3 are set to a cut-off state. After the line switch 21 is switched to a cut-off state, for example, in case there is an access to the WAN 3 from the computers 11 in the LAN 1, the control part 22 can send a control signal to the line switch part 21 so that a connection state is reset. Also, the control part 22 can control the line switch part 21 to switch it to a cut-off state, even when the above-mentioned various events are generated, in addition to the case where the alarm generation part 24 generates an alarm.

[0036] With this constitution, in case there is an illegal access to the computer 11 in the LAN 1 from the WAN 3, since not only the illegal access is not transferred by the firewall 2 but the line switch part 21 is set to a cut-off state, the prevention of the illegal access can be more reinforced. Thus, a higher-security system can be constructed, compared with the system shown in the above-mentioned embodiment.

[0037] In the above-mentioned embodiment, the network connection system in which the LAN 1 is used as an internal network and the WAN 3 as an external network is connected to it has been explained as an example. However, for example, even in a network system in which LAN and LAN are connected by router, etc., the above-mentioned line switch part 21 and control part 22 can be installed in one or more LAN among them.

[0038]

(Effects of the invention)

As explained above, according to the present invention, each computer connected to an internal computer can be prevented from an illegal access from an external network, and data can be exchanged in the internal network without trouble.

Brief description of the figures

Figure 1 is a block diagram showing the constitution of the network connection system in an embodiment of the present invention.

Figure 2 is a block diagram showing the constitution of the network connection system in another embodiment of the present invention.

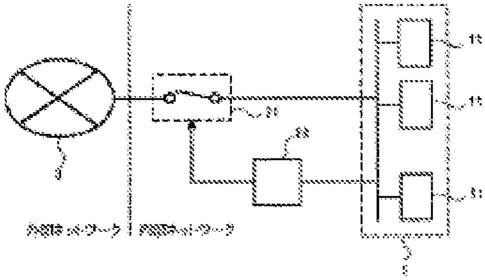
Figure 3 is a block diagram showing the constitution of the network connection system in another embodiment of the present invention.

Figure 4 is a block diagram showing a network interface module with a security switch of a conventional example.

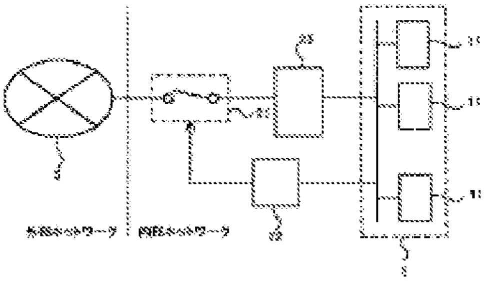
Explanation of numerals:

1	LAN
2	Firewall
3	WAN
11	Computer
21	Line switch part
22	Control part
23	Firewall
24	Alarm generation part

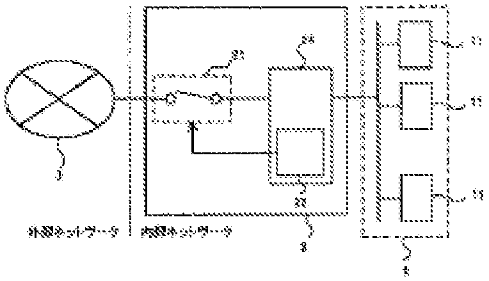
【図1】



【図2】



【図3】



【図4】

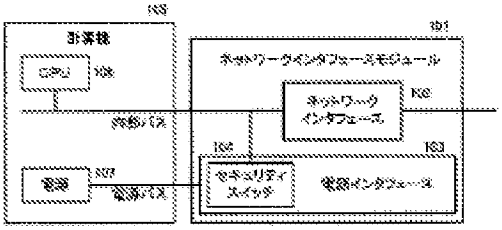


Figure 1:

1. External network

2. Internal network

Figure 2:

1. External network

2. Internal network

Figure 3:

1. External network

2. Internal network

Figure 4:

101	Network interface module
102	Network interface
103	Power source interface
104	Security switch
105	Computer
107	Power source
A.	Internal bus
B.	External bus